



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/521,429

01/13/2005

Haim Engler

SSXG 1031689

8952

27111

7590

11/07/2007

GORDON & REES LLP
101 WEST BROADWAY
SUITE 1600
SAN DIEGO, CA 92101

EXAMINER

TRAORE, FATOUMATA

ART UNIT

PAPER NUMBER

2136

MAIL DATE

DELIVERY MODE

11/07/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/521,429

Applicant(s)

ENGLER ET AL.

Examiner

Fatoumata Traore

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 13 January 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 13 January 2005 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>03/28/2005</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This action is in response of the original filing of January 13th, 2005. Claims 1-12 are pending and have been considered below.

Claim Objections

2. Claim 1 is objected to because of the following informalities: the preamble of claim 1 recites *"In a wireless network comprising a server and server software including an intelligent software agent, a method of automatically providing a secure connection between the wireless network and a user-operated device seeking access to the wireless network, the method comprising:"* It is unclear to the examiner if applicant is claiming a system or a method. Appropriate correction is required.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1, 2 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen et al (US 2001/0041556) in view of Christmas (US 6,085,084).

Claim 1: Laursen et al discloses a wireless network comprising a server and server software including an intelligent software agent, a method of automatically

providing a secure connection between the wireless network and a user-operated device seeking access to the wireless network (Fig. 2a), the method comprising:

- i. In response to an initial request for access to the wireless network by the device (*wherein the provisioning interface receives a request to push the fleet data in the memory to the plurality of the mobile stations*) (paragraphs [0016], [0019])
- ii. Automatically installing the software agent on the device (*the request prompts a challenge response from provisioning interface 202*) (paragraph [0055]);
- iii. Executing the software agent on the device to gather information from the requesting device, including device information and user authentication information (*executing the request to cause the fleet data pushed by the proxy server module to the plurality of the mobile stations*) (paragraphs [0028], [0038], [0055]),
- iv. Transmitting the device identification and user authentication information to the server (*Provisioning interface 202 returns a challenge for the entry of a set of predefined credential information, such as a username or a corresponding password, when the fleet data request to a fleet of mobile stations is made from the fleet manager terminal*) (paragraph [0056]); and

v. Verifying the device identification and user authentication information wherein when successfully verified (*At 710, the received credential information is verified by a comparison against corresponding predefined credential information*) (paragraphs [007], [0056]), storing the identification and authentication information on an authorized access list (*the business must be in the list of authorized entities so as to be able to access the fleet managing system*) (paragraph [0054]), providing a unique encryption key to the device for storage thereon (*Meanwhile commanding mobile station 520 and proxy server 510 exchange encrypt keys and authenticate each other to generate a session key according to a mutually acceptable encryption scheme*)(paragraph[0070] and granting the requesting device access to the wireless network(*otherwise a trust is therefore established between the provisioning entity and the provisioning interface. At 712, the fleet data request from the provisioning entity is granted*)(paragraph [0079]); and when unsuccessfully verified (*If there is a disagreement or mismatch between the supplied credential information and predefined credential information, the original request from the provisioning entity is discarded*) (paragraph [0079]), storing the identification and authentication information on an unauthorized access list and denying the device access to the wireless network.

But does not explicitly discloses a step of storing the identification and authentication information on an unauthorized access list.

However Christmas discloses an automated creation of list of disallowed network points for use in connection blocking which further discloses:

- vi. Storing the identification and authentication information on an unauthorized access list (Fig. 1, item 114).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store a list of unauthorized user in Laursen et al's disclosure. One would have been motivated to do so in order to identify unauthorized network access attempts as discloses by Christmas (abstract).

Claim 2: Laursen et al and Christmas disclose a wireless network as in claim 1 above, and Laursen et al further disclose that the method further comprising, in response to a subsequent request for access to the wireless network by the device (*wherein the provisioning interface receives a request to push the fleet data in the memory to the plurality of the mobile stations*) (paragraphs [0016], [0019]) –

- i. Receiving the unique key corresponding to the device (*Each of the mobile stations is assigned a device ID 402*) (paragraph [0062], [0066]);
- ii. Retrieving the identification and authentication information corresponding to the unique key (*In other words, the user accounts can be kept in a database that is physically placed in any computing device coupled to proxy server 230 and can be collected or fetched therefrom*) (paragraphs [0064], [0066]);

iii. Comparing the identification and authentication information with the authorized and unauthorized lists (*the received credential information is verified by a comparison against corresponding predefined credential information*) (paragraph [0079]); and

iv. Based on the comparison, one of granting and denying the device access to the wireless network (*If there is a disagreement or mismatch between the supplied credential information and predefined credential information, the original request from the provisioning entity is discarded otherwise a trust is therefore established between the provisioning entity and the provisioning interface*) (paragraph [0079]).

5. Claims 3, 4, 8, 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen et al (US 2001/0041556) in view of Christmas (US 6,085,084) as applied to claim 1 above in further view of Mehring et al (US 6,609,115).

Claim 3: Laursen et al and Christmas disclose a wireless network as in claim 1 above, while neither of them explicitly discloses that the step of denying access comprises generating a notification message that an unauthorized device has attempted to access the network. However, Mehring et al discloses a method for limited online access to restricted documentation, which further discloses that the step of denying access comprises generating a notification message that an unauthorized device has attempted to access the network (*If the password is not authentic, the addressed web server will send an error message to the remote*

system)(column 9, lines 53-67). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al and Christmas of such send a notification message. The motivation of doing so would have been to limit access to such restricted and highly sensitive data as disclosed by Mehring et al (column 1, lines 51-67).

Claim 4: Laursen et al and Christmas disclose a wireless network as in claim 1 above, while neither of them explicitly discloses that the step of granting access comprises providing access in accordance with existing network access rights of the user operating the device. However, Mehring et al discloses a method for limited online access to restricted documentation, which further discloses that the step of granting access comprises providing access in accordance with existing network access rights of the user operating the device (*Based on the criteria and variable data retrieved during the authorization step 168, the policy server 114 determines whether the requesting remote system user has access rights to the requested software application 170*)(column 9, lines 53-67; column 10, lines 1-31). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al and Christmas of such to provide access based on user access right. The motivation of doing so would have been to limit access to such restricted and highly sensitive data as disclosed by Mehring et al (column 1, lines 51-67).

Claim 8: Laursen et al and Christmas disclose a wireless network as in claim 1 above, while neither of them explicitly discloses that the step of automatically

installing application software on the device. However, Mehring et al discloses a method for limited online access to restricted documentation, which further discloses that the step of automatically installing application software on the device (*The license server 144 generates licenses, installs the generated licenses on the remote systems 12 via the network 80, and logs the licenses into the policy/license database 146*)(column 12, lines 30-53). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al and Christmas of such to automatically install application software. The motivation of doing so would have been to limit access to such restricted and highly sensitive data as disclosed by Mehring et al (column 1, lines 51-67).

Claim 11: Laursen et al and Christmas disclose a wireless network as in claim 1 above, while neither of them explicitly discloses that the step of granting access further comprises conformity to a security policy with respect to access from multiple devices. However, Mehring et al discloses a method for limited online access to restricted documentation, which further discloses that the step of granting access further comprises conformity to a security policy with respect to access from multiple devices (*Based on the criteria and variable data retrieved during the authorization step 168, the policy server 114 determines whether the requesting remote system user has access rights to the requested software application 170*)(column 9, lines 53-67; column 10, lines 1-31). It would have been obvious to one of ordinary skill in the art at the time the invention was made

to modify the combined network Laursen et al and Christmas of such to provide access based on user access right. The motivation of doing so would have been to limit access to such restricted and highly sensitive data as disclosed by Mehring et al (column 1, lines 51-67).

6. Claims 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen et al (US 2001/0041556) in view of Christmas (US 6,085,084) as applied to claim 1 above in further view of Weigand (US 7,151,938).

Claim 5: Laursen et al and Christmas disclose a wireless network as in claim 1 above, while neither of them explicitly discloses that the step of determining the geographical location of the device. However, Weigand discloses a dynamically managing and reconfiguring wireless mesh network which further discloses a step of collecting information relevant for billing the user for services accessed through the network (*the wireless base station controller may access a geo-location database that correlates billing addresses with positioning information to determine which base station lobes are accessible*)(column 16, lines 38-52). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al and Christmas of such to provide information related to billing. The motivation of doing so would have been to limit access to such restricted and highly sensitive data.

Claim 6: Laursen et al and Christmas disclose a wireless network as in claim 1 above, while neither of them explicitly discloses that the step of collecting information relevant for bandwidth allocation over the network. However, Weigand discloses a dynamically managing and reconfiguring wireless mesh network, which further discloses the step of collecting information relevant for bandwidth allocation over the network (*Reconfiguring the wireless network may include changing bandwidth allocated to a subscriber system participating in the lobe pool in the wireless network*) (column 16, lines 38-52). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al and Christmas of such to provide information related bandwidth. The motivation of doing so would have been to limit access to such restricted and highly sensitive data.

7. Claims 7 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen et al (US 2001/0041556) in view of Christmas (US 6,085,084) as applied to claim 1 above in further view of Bade et al (US 6,898,628).

Claim 7: Laursen et al and Christmas disclose a wireless network as in claim 1 above, while neither of them explicitly discloses that the step of determining the geographical location of the device. However, Bade et al discloses a method for providing positional authentication, which further discloses that the step of determining the geographical location of the device (*The system 100 also includes a positioning system 110 that includes at least one transmitter 112, such*

as a positioning satellite. The positioning system 110 can be any suitable positional access system, such as satellite, microwave, infrared, or radio based, which provides positional access with any suitable method) (column 3, lines 48-58). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al and Christmas of such to determine the geographical location. The motivation of doing so would have been to automatically prevents unauthorized access to the extranet based on locations where access is not allowed on the client machine as disclosed by Bade et al (column 2, lines 16-26).

Claim 10: Laursen et al and Christmas disclose a wireless network as in claim 1 above, while neither of them explicitly discloses that the network comprises an isolated network segment and the initial connection between the device and the network is limited to the isolated network segment. However, Bade et al discloses a method for providing positional authentication, which further discloses wherein the network comprises an isolated network segment and the initial connection between the device and the network is limited to the isolated network segment (*For instance, an administrator of a host server that contains sensitive and secure data for numerous users located throughout a country, such as the Social Security Office, can restrict access by location with the present invention*) (column 5, lines 26-36). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al and Christmas of such to restrict access to the device. The

motivation of doing so would have been to automatically prevents unauthorized access to the extranet based on locations where access is not allowed on the client machine as disclosed by Bade et al (column 2, lines 16-26).

8. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen et al (US 2001/0041556) in view of Christmas (US 6,085,084) as applied to claim 1 above in further view of Limsico (US 6,662,228).

Claim 9: Laursen et al and Christmas disclose a wireless network as in claim 1 above, while neither of them explicitly discloses that wherein the encryption key is a certificate. However, Limsico discloses an internet server authentication client, which further discloses that the encryption key is a certificate (column 4, lines 1-15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al and Christmas of such to provide the certificate as the encryption key. The motivation of doing so would have been to transmit data between machines securely, without possibility of interception or spoofing as disclosed by Limsico (column 1, lines 60-65).

9. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Laursen et al (US 2001/0041556) in view of Christmas (US 6,085,084) as applied to claim 1 above in further view of Bagshaw (US 7,089,426).

Claim 12: Laursen et al and Christmas disclose a wireless network as in claim 1 above, while neither of them explicitly discloses that the user is defined as a guest user and given a temporary encryption key with guest network access rights. However, Bagshaw discloses a method of encryption, which further discloses wherein the user is defined as a guest user and given a temporary encryption key with guest network access rights (column 4, lines 21-38). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined network Laursen et al and Christmas such as to provide a temporary encryption key. The motivation of doing so would have been to limit access to such restricted and highly sensitive data.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Art Unit: 2136

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Friday November 2nd, 2007

Nassar G. Moazzami
Supervisory Patent Examiner


11/5/07